NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 1 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19, 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

PURPOSE

The purpose of this policy is to establish requirements for reporting, documenting, and investigating incidents and complaints resulting from suspected violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the North Carolina (NC) Identity Theft Protection Act, or the department's privacy practices, policies or procedures regarding confidential information.

This policy applies to the following DHHS agencies: Agencies covered by HIPAA; Agencies covered by the NC Identity Theft Protection Act; and Agencies that generate, use, collect, disclose or store confidential information.

POLICY

DHHS agencies shall immediately report, investigate, and document all suspected privacy incidents or complaints electronically, ensuring that all required documents are attached to the electronic report. Although the incident or complaint reporting process to the DHHS Privacy and Security Office (PSO) is now electronic, agencies may accept incidents or complaints from DHHS workforce members and individuals using the revised DHHS Privacy Incident Report or DHHS Privacy Complaint Report form to document the incident or complaint and retain these documents for the agencies' future reference. It is not necessary to attach these documents to the electronic report, however.

DHHS agencies shall develop procedures to respond to incidents or complaints whenever there is reason to believe that an agency's privacy practices, policies or procedures have been breached in some manner. Privacy incidents or complaints shall be resolved in a timely manner, ensuring clients and other individuals that the department is committed to protecting their confidential information.

Each agency shall designate a staff member who is responsible for communicating and assisting workforce members or individuals who have questions or concerns, or who wish to file incidents or complaints regarding the agency's privacy practices. When reporting incidents or complaints electronically, the agency shall report its internal incident or complaint number, incident

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 2 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19**,** 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

classification and severity, investigative analysis of the facts, description of the corrective actions taken, and mitigation efforts undertaken. The report shall be updated using the ticket tracking ID number, which is generated after submitting the incident or complaint until the investigation is completed and closed. In addition, any privacy incident or complaint that includes a disclosure for which an accounting is required must be documented and entered into the accounting of disclosures logs.

Background

The department requires that its agencies develop procedures for reporting incidents and complaints and for responding to individuals who make inquiries, express concerns, and/or file complaints regarding the agency's privacy practices, policies, and procedures. Such communications may be rendered:

1. In person;
2. In writing (letter/e-mail/fax); or • By telephone.

DHHS agencies shall respond to every identifiable privacy incident or complaint received. Each identifiable privacy incident or complaint shall generate an investigation, determination and a response. Ensuing investigations should focus on both the specific privacy incident or complaint and any patterns of similar privacy incidents or complaints.

Documentation of privacy incidents or complaints, investigative efforts, and incident or complaint determinations are considered administrative information and shall be maintained in administrative files for at least six (10) years. Documentation of privacy incident or complaint information shall not be filed in a client's treatment, financial, or other designated record sets.

IMPLEMENTATION

NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 3 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19**,** 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

DHHS agencies shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident or a complaint.

Reporting Incidents and Complaints

1. Communication Methods

   Incidents: A DHHS workforce member, business associate or vendor shall report incidents to the agency's Privacy Official or Privacy Coordinator. The Privacy Official or Privacy Coordinator shall then report the incident to the DHHS PSO electronically.

   Complaints: An individual can file a complaint with the agency directly, or with the department's Privacy Officer. The DHHS Privacy and Security Office is responsible for maintaining a current list of designated privacy contacts in each agency and; therefore, each agency is required to notify the DHHS Privacy and Security Office of any staff changes in their privacy official or privacy coordinator positions.

   Agency: An individual may file a privacy complaint in person, in writing or by telephone directly with an agency. The Privacy Official or Privacy Coordinator shall immediately notify the complainant in writing that the agency has received his/her complaint, is investigating it and will notify the complainant of its resolution. DHHS agencies shall not retaliate against any individual for filing a HIPAA privacy complaint with either the agency, the department, or the Secretary of the US Department of Health and Human Services

   Department's privacy officer: An individual may file a complaint with the DHHS Privacy and Security Office if, for some reason, the individual does not wish to speak to the agency Privacy Official or Privacy Coordinator. Such communication may be accomplished in person, in writing, or by telephone. If an individual contacts the DHHS Privacy and Security Office before an agency, the DHHS Privacy and Security Office

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 4 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19, 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

shall determine if the issue is agency-specific and shall attempt to refer the individual to the appropriate agency, as needed. If the individual does not wish to speak with agency staff directly, the DHHS Privacy and Security Office shall collect the complaint information and work with the agency Privacy Official or Privacy Coordinator to resolve the issue.

Documenting, Investigating, and Resolving Incidents and Complaints:

1. Documentation

   All complaints can be entered into the incident reporting system. It is located at https://security.ncdhhs.gov/

   The DHHS agency shall document all telephone complaints and direct complainant to the Incident reporting site so that the event shall be investigated as an incident.

2. Investigation and Resolution

   Investigation of privacy incidents or complaints must begin immediately following receipt of an expressed incident or complaint. Investigative actions and resolution shall be documented electronically using the link https://security.ncdhhs.gov/ .

   Once a ticket is entered into the incident reporting system, the appropriate privacy or security official is assigned to investigate the allegation. It is important to provide detailed information, including dates, locations, titles, types of identifiers involved and attach documents, since this will be the DHHS agency's main record of the investigation.

3. Responsibility of Privacy Official or Privacy Coordinator

   Each agency shall determine its procedures for investigating and resolving privacy incidents or complaints. However, each agency must designate an individual as Privacy Official (if covered by HIPAA) and/or as Privacy Coordinator (if not covered by HIPAA),

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 5 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19**,** 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

who will be responsible for reporting, investigating and documenting privacy incidents or complaints.

If an individual reaches out to the agency directly, the agency's Privacy Official or Privacy Coordinator shall determine if the issue can be resolved at the agency level. If so, the Privacy Official or Privacy Coordinator shall be responsible for investigating and documenting the concern until the issue is resolved. Agencies operated by the Division of State Operated Healthcare Facilities are encouraged to involve their internal client advocates in the complaint investigation process when deemed appropriate.

If the Privacy Official or Privacy Coordinator determines the issue involves other agencies in the department or if he/she is unable to obtain resolution at the agency level, the issue shall be forwarded to the DHHS Privacy and Security Office.

4. DHHS Privacy and Security Office Review

   The DHHS Privacy and Security Office shall review the reporting, documentation and resolution of all privacy incidents or complaints. If the agency has not resolved the incident within a reasonable time, the DHHS Privacy and Security Office shall involve anyone determined to be necessary to assist in resolution of the incident or complaint, including the Attorney General's Office. If the DHHS Privacy and Security Office has comments, suggestions, questions, etc. about the investigation and resolution of the incident or complaint, he or she shall document this information within the report for consideration by the agency.

5. Training

   Whenever a privacy incident or complaint has occurred, the DHHS agency must evaluate the occurrence to determine if additional staff training is necessary. Depending upon the situation, it may be determined that the entire agency should receive training that is specific to the privacy incident or complaint. The Privacy Official or Privacy Coordinator shall review any privacy training developed as part of the privacy incident or complaint

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 6 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19, 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

resolution to ensure the scope of the training adequately addresses the subject of the incident and reinforces the DHHS and agency privacy practices, policies and procedures.

Types of Incidents and Complaints

Currently, there are three types of privacy incidents or complaints: HIPAA, NC identity theft, and departmental practice, policy or procedure violations. There may be times when these three types of privacy incidents or complaints overlap, and agencies are unsure about whether any given event could be considered a breach of unsecured PHI, a security breach, a departmental practice, policy or procedure violation, or a combination thereof. In these instances, please contact the DHHS Privacy and Security Office for guidance.

1. HIPAA incidents and complaints (breach of unsecured PHI)

   The **HIPAA Breach Notification for Unsecured PHI policy** outlines the procedures HIPAA covered DHHS agencies should follow when they evaluate and report an unauthorized acquisition, access, use, or disclosure of protected health information (PHI). These procedures include information about to whom an impermissible acquisition, access, use, or disclosure of PHI should be immediately reported, who should be involved in determining if a breach of unsecured PHI has occurred and if the affected individual(s) should be notified.

   HIPAA covered agencies which become aware of an unauthorized acquisition, access, use, or disclosure of PHI shall **immediately** notify the DHHS Privacy and Security Office (PSO) by reporting the incident or complaint to the following link: https://security.ncdhhs.gov/ and complete the applicable sections .

2. NC Identity Theft Protection Act incidents and complaints (security breach)

   The **Identity Theft and Security Breach Notification policy** outlines the procedures all DHHS agencies should follow when they report a disclosure or possible disclosure of

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 7 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19, 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

identifying information. These procedures will include information to whom a disclosure or possible disclosure of identifying information should be immediately reported; who should be involved in determining if a security breach has occurred and if the affected persons should be notified. Any DHHS agency which becomes aware of a disclosure or possible disclosure of identifying information shall **immediately** notify the DHHS PSO by reporting the incident or complaint to the following link: https://security.ncdhhs.gov/ and complete the applicable sections.

3. Departmental policy or procedure violation incidents or complaints.

   There are DHHS agencies that maintain confidential information but are not covered by HIPAA. The Privacy Safeguards policy specifically addresses how divisions and offices should protect confidential information from unauthorized use or disclosure.

   Any DHHS agency which becomes aware of an unauthorized use or disclosure of confidential information shall **immediately** notify the DHHS PSO by reporting the incident or complaint to https://security.ncdhhs.gov/

4. Overlapping incidents and complaints

There may be instances when overlapping issues arise and agencies are unsure about whether any given event could be considered a HIPAA privacy incident, a security breach, or a combination thereof. There could also be situations where privacy and security incidents overlap. When evaluating incidents or complaints, the Privacy Official or Privacy Coordinator should look for key words such as “health information”, “SSN”, or “laptop”, and consider how these words might suggest which type of incident or complaint to report.

NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Privacy Incident and Complaint Reporting
PAGES: 8 of 8	**REPLACES POLICY DATED:** 9/30/18
CURRENT EFFECTIVE DATE: 11/1/19	**ORIGINAL EFFECTIVE DATE:** 4/14/03
REVISED DATE: 11/1/19 **REVIEW DATE:** 11/1/19	**APPROVED DATE:** 11/1/19**,** 4/14/03
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

EXAMPLE: There can be differences and similarities between a [security] incident reportable to ITS, a security breach and a breach of unsecured PHI. If a DHHS-issued laptop is stolen from a hotel, this event should be reported as a [security] incident to the DHHS PSO, since an information technology resource has been accessed or used without authorization. Whether this event is also a breach of unsecured PHI will depend upon whether the stolen laptop contained PHI (i.e. a type of health information together with an identifier). The "Privacy Risk Assessment" form should be completed to determine whether notification of the affected client(s) is required. Whether the DHHS agency will have to notify affected persons will depend upon whether the laptop was encrypted or another exception to the notification rule exists. If PHI was present, the unauthorized access posed a significant risk of financial, reputational, or other harm to the individual, and no exception exists, the agency will have to notify. In addition, if the event involves "personal information" and the laptop was not encrypted, this event could also be a security breach.

ENFORCEMENT

For questions or clarification on any of the information contained in this policy, please contact the DHHS Privacy and Security Office. For general questions about department-wide policies and procedures, contact the DHHS Policy Coordinator.